



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/787,029	03/13/2001	Takuya Hirano	010294	8139

38834 7590 08/02/2004

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON, DC 20036

EXAMINER

AKPATI, ODAICHE T

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 08/02/2004

6

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/787,029

Applicant(s)

HIRANO, TAKUYA

Examiner

Tracey Akpati

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 13 March 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 003.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Werner et al (Eavesdropping using quantum-nondemolition measurements).

With respect to Claim 1, Werner et al meets the limitation of “a quantum cipher communication system characterized by the step of detecting eavesdropping based on a change in a quantum-mechanical probability distribution defined by an amplitude and a phase in a difference signal derived from a signal light which change is produced by an eavesdropping operation” on page 639 and 640, column 1. The joint detection probabilities for both polarizer one and two depend on phase and amplitude of the signal. The eavesdropping operation is represented by the quantum-nondemolition measurement of photon number. The recombined beams on page 640, column 1 represent the difference signal.

It would have been obvious to one of ordinary skill in the art at the time of the invention to assume the recombined beams to be the difference signal because the recombined beams are derived from an orthogonally polarized light beam that is split in two. Furthermore, the polarization directions are chosen by the eavesdropper.

Claims 2, 5, 8-11, 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Werner et al (Eavesdropping using quantum-nondemolition measurements) in view of Bethune (6188768 B1).

With respect to Claim 2, all the limitation is met by Werner et al except for the following limitation.

Bethune meets the limitation of “splitting a light signal from a transmission source side into an intense reference signal and a weak transmission signal which is so weak that a change in its quantum mechanical state is detectable” on column 2, lines 28-37; and “imparting a phase difference between said reference signal and said transmission signal while they are in a process of transmission” on column 2, lines 28-37. They are orthogonally polarized and hence are imparted a specific phase difference. Further limitation of “superimposing in a transmission receiving side said reference signal and said transmission signal to form two output lights which are opposite in phase and producing a difference signal which is represented by a difference between said two output lights” on column 2, lines 28-37; and “deriving a frequency distribution of said difference signal as a function of a fluctuation of the quantum state of said transmission signal based upon or in accordance with the frequency distribution of said difference signal, making privacy (secret) keys respectively at said transmission source and receiving sides or holding in common thereby” inherently on column 2, lines 51-57 and abstract, last sentence. The key after being decoded is communicated to the other receiving party. Further limitation of “directly observing the fluctuation of the quantum state of said transmission signal” on column 2, lines 51-57 and column 5, lines 61-64.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the system of Werner et al so as to enable a secure key distribution system between two parties.

With respect to Claim 5, all the limitation is met by Werner et al except for the following limitation.

Bethune meets the limitation of “characterized in that said reference signal and said transmission signal are split both in time and as polarized and then transmitted to travel along a common path” in the abstract.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the system of Werner et al so as to enable a secure key distribution system between two parties.

With respect to Claim 8, Werner et meets all the limitation except the following limitation. The limitation of “characterized in that threshold values are established, respectively, for positive and negative values of said difference signal, and that the state of said transmission signal is discriminated on the basis of said threshold values” by Bethune on column 7, lines 32-46.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the system of Werner et al so as to enable a secure key distribution system between two parties.

With respect to Claim 9, all the limitation is met by Werner et al except the following limitation. The limitation of “characterized in that in addition to the phase modulations designed to transmit privacy keys, such a phase modulation is so imparted as described and having a value later determined for making a correction for a fluctuation of the difference in optical path between said reference signal and said transmission signal which develops by reason of an external cause” is met by Bethune on column 7, lines 32-46.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the system of Werner et al because the fluctuation in the difference signal by an external cause determines if an eavesdropper has gained access to the communication.

With respect to Claim 10, all the limitation is met by Werner et al except the following limitation.

The limitation of “characterized in that such phase modulations are so imparted as described and including those for transmitting privacy keys and those with values later determined are randomly repeated” is met by Bethune on column 6, lines 6-28.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the system of Werner et al because introducing a randomness into the transmission process for key generation makes the generated key harder to guess by an attacker.

With respect to Claim 11, all the limitation is met by Werner et al except the following limitation.

The limitation of “characterized in that eavesdropping is detected on the basis of an increase in the error rate of said difference signal” is met by Bethune on column 5, lines 64-67 and on column 6, lines 1-5.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the system of Werner et al because detection of an eavesdropper allows the user to know that the keys are no longer secure and are to be discarded.

With respect to Claim 13, all the limitation is met by Werner et al except the following limitation.

The limitation of “characterized in that said two output lights are converted into corresponding electric signals through photoconductor diodes” is obvious over Bethune, Fig. 3A and 3B.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the system of Werner et al because conversion of the light signal to an electric signals allows the system to be able to measure the difference signal so as to decipher if the signal has been eavesdropped.

With respect to Claim 14, all the limitation is met by Werner et al except the following limitation.

The limitation of “characterized in that for said photoconductor diodes, use is made of silicon photoconductor diodes when the light has a wave length of 600 nm to 900 nm, and of InGaAs photoconductor diodes when the light has a wave length of 1000 nm to 1500 nm” is obvious over Bethune on column 4, lines 39-43, 66-67 and column 5, lines 1-6.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bethune within the system of Werner et al because conversion of the light signal to an electric signals allows the system to be able to measure the difference signal so as to decipher if the signal has been eavesdropped.

Claims 3, 4, 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bethune (6188768 B1).

With respect to Claim 3, Bethune meets the limitation of “a first beam splitter for splitting a light from a light source into a transmission signal and a reference signal” on column 2, line 67 and column 3, lines 1-2. The light is split into two signals and because these signals are polarized orthogonally, this makes splitting of the beams into a transmission and a reference signal obvious. Bethune meets further limitation of “a phase modulating means for imparting a phase modulation to said transmission signal” on column 2, lines 63-67; and “a light attenuator for converting said transmission signal into a weak transmission signal which is so weak that a change in its quantum state is detectable” on column 5, lines 45-51. By scattering the light pulse, a weaker signal emerges. Further limitation of “a phase modulating means for imparting a phase

Art Unit: 2135

modulation to said reference signal, said system also including, operative after a relative phase difference is imparted between said transmission and reference signals” is met in the abstract; and “a second beam splitter for superimposing said phase modulated weak transmission signal and said phase modulated intense reference signal to form two output lights” on column 5, lines 32-41. PBS1 and PBS2 are the two beam splitters. Bethune meets the limitation of “a first and a second photoelectric conversion elements for converting said two output lights from said second beam splitter into two corresponding electric signals which are opposite in phase” on column 6, lines 6-14; and “an amplifier for amplifying a difference signal representative of a difference between said two output lights to output an amplified corresponding voltage” on column 6, lines 20-28 and 1-5. The difference signal is represented by the combined signals. The amplifier is represented by the power meter monitor because it detects a difference in both signals and decides if the signal has been eavesdropped.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have an amplifier present in the invention because the presence of an amplifier within the power meter monitor will amplify the difference signal so that the signal can be accurately measured to determine if it has been eavesdropped.

With respect to Claim 4, Bethune meets the limitation of “characterized in that said phase modulating means includes a mirror movable by a distance as small as the wave length of an incident light” on column 1, lines 43-53, column 2, lines 5-12 and 58-63.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the Faraday mirror be adjustable by the distance as small as the wavelength of an

Art Unit: 2135

incident light because this would enable the mirror be able to polarize the light pulse as accurately as it does. The faraday mirror introduces a change in phase of the light pulse.

With respect to Claim 6, Bethune meets the limitation of “a first beam splitter for splitting a light from a light source into a transmission signal and a reference signal” on column 2, line 67 and column 3, lines 1-2; and “a first light polarizes for polarizing said transmission signal through longer one of two distance paths” on column 2, lines 37-42, 45-48 and 51-57; and “a light attenuator for converting said transmission signal into a weak transmission signal which is so weak that a change in its quantum state is detectable” on column 5, lines 45-51. The scattering of the light pulse inherently weakens it. Bethune meets further limitation of “a first phase modulating means for imparting a predetermined phase modulation to said transmission signal and a first polarized beam splitter for receiving said intense reference signal having passed through shorter one of two distance paths and said transmission, signal and returning the received signal to travel along a common optical path, said system also including, operative after a relative phase difference is imparted between said transmission and reference signals and included in a transmission receiving side” on column 5, lines 32-44; and “a second polarized beam splitter for isolating from each other said transmission and reference signals transmitted through a single optical fiber” on column 5, lines 32-33; and “a second phase modulating means for imparting a phase modulation to said isolated transmission signal through shorter one of two distance paths” on column 2, lines 42-48; and “a second light polarizer for polarizing said isolated reference signal through longer one of two distance paths” on column 5, lines 32-41; and “said system further including a second beam splitter for superimposing said transmission and

Art Unit: 2135

reference signals which are coincident with each other in time and polarization to produce two output lights” on column 4, lines 53-54 and column 5, lines 32-41. PBS2 is the second beamsplitter. Further limitation of “a first and a second photoelectric conversion elements for converting said two output lights into corresponding electric signals which are opposite in phase” is met on column 6, lines 6-14; and “an amplifier for amplifying a difference signal representative of a difference between said two output lights to output an amplified corresponding voltage” is met on column 6, lines 20-28 and 1-5. The difference signal is represented by the combined signals. The amplifier is represented by the power meter monitor because it detects a difference in both signals and decides if the signal has been eavesdropped.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have an amplifier present in the invention because the presence of an amplifier within the power meter monitor will amplify the difference signal so that the signal can be accurately measured to determine if it has been eavesdropped.

With respect to Claim 7, Bethune meets the limitation of “characterized in that a third light polarizes is provided in an output side of said optical fiber for making a correction for a disturbance of polarization of said reference signal” on column 5, lines 32-38.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Werner et al (Eavesdropping using quantum-non demolition measurements) in view of Bartelt et al (The Wigner Distribution Function—An Alternative Signal Representation in Optics).

With respect to Claim 12, all the limitation is met by Werner et al except for the following limitation.

The limitation of “characterized in that eavesdropping is detected on the basis of a change in a Wigner distribution function that indicates a quantum mechanical state of said difference signal” is met by Bartelt et al on page 260.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bartelt et al within the system of Werner because the Wigner distribution function is an effective way to determine if the signal has been eavesdropped.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 703-305-7820. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 09/787,029

Page 12

Art Unit: 2135

OTA

Handwritten signature
AU 2135